UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/698,197	10/31/2003	Pradipta Kumar Banerjee	JP920030162US1	9974

39903 7590 04/03/2008

IBM ENDICOTT (ANTHONY ENGLAND)
LAW OFFICE OF ANTHONY ENGLAND
PO Box 5307
AUSTIN, TX 78763-5307

EXAMINER	
OSMAN, RAMY M	
ART UNIT	PAPER NUMBER
2157	

MAIL DATE	DELIVERY MODE
04/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/698,197	BANERJEE ET AL.	
	Examiner	Art Unit	
	RAMY M. OSMAN	2157	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 December 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-4,7,9-11,13-16,19-23,25-28,31,33 and 34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4,7,9-11,13-16,19-23,25-28,31,33 and 34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is responsive to amendment filed on December 27, 2007, where applicant amended claims 1,2,11,13,14,19,23,25,26,27,28,31,33,34 and cancelled claims 5,6,8,17,18,29,30,32. Claims 1-4,7,9-11,13-16,19-23,25-28,31 and 33-34 are pending.

Response to Arguments

2. Applicant's arguments, filed 12/27/2007, with respect to the rejection(s) of claim(s) 1-4,7,9-11,13-16,19-23,25-28,31 and 33-34 have been fully considered and are persuasive. The previous rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of **Tarquini et al (US Patent Publication No 2003/0101353),** as outlined below. Applicants arguments are therefore moot in view of the new grounds of rejection.

3. Previous claim objections, 101 rejections and 112 rejections are withdrawn.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. **Claims 1,3-11,13,15-23,25 and 27-34 rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini et al (US Patent Publication No 2003/0101353) in view of Copeland (US Patent No 7,185,368)**.

6. In reference to claim 1, Tarquini teaches a method of detecting an intrusion in a communications network, the method comprising the steps of:

scanning data packets by a first computer system to which the data packets are directed, wherein the scanning includes the computer system processing the packets by a transport layer of a network protocol associated with said communications network using signatures from a repository of said signatures (¶ 30 lines 25-30);

determining if said scanned data packets are malicious (¶ 30 lines 30-32); and

taking at least one action if any of the data packets are determined to be malicious (¶ 30 lines 30-32),

to provide a queue for data from the data packets to a first application on the first computer system, wherein the scanning of the respective data packets occurs before the first application receives the data from the respective data packets (Figure 6 and middle of ¶ 38 and ¶s 39-40, Tarquini discloses queuing data through a network stack for performing intrusion prevention at each network layer).

Tarquini fails to explicitly teach the limitations wherein at least one application receive queue (ARQ) functions intermediate said transport layer and an application layer of the first computer system provides the queue for data, and wherein said scanning step is selected from the group consisting of: scanning between said transport layer and said at least one ARQ; and scanning the data packets from said at least one ARQ. However, Holland teaches host-based

monitoring of a network protocol stack (column 5 lines 23-45). Holland discloses monitoring via queues intermediate application and transport layers for providing and scanning data for intrusion detection, and further discloses scanning between the TCP layer (Figure 4 and column 6 lines 35-61).

It would have been obvious for one of ordinary skill in the art to modify Tarquini wherein at least one application receive queue (ARQ) functions intermediate said transport layer and an application layer of the first computer system provides the queue for data, and wherein said scanning step is selected from the group consisting of: scanning between said transport layer and said at least one ARQ; and scanning the data packets from said at least one ARQ as per the teachings of Holland for the purpose of implementing intrusion detection on the network protocol stack level.

7. In reference to claim 3, Tarquini teaches the method according to claims, further comprising the step of transmitting to said application layer any data packets determined not to be malicious (¶ 40-41).

8. In reference to claim 4, Tarquini teaches the method according to claim 1, wherein said scanning and determining steps are implemented using a scan module (¶ 40-41).

9. In reference to claim 7, Tarquini teaches the method according to claim 6, further comprising the step of obtaining data from said at least one application receive queue (ARQ) (Holland, Figure 4 and column 6 lines 35-61, see rationale for claim 1 above).

10. In reference to claim 9, Tarquini teaches the method according to claim 1, further comprising the step of dispatching said data packets to one or more handlers for scanning, if said protocol is monitored (¶ 40-41).

11. In reference to claim 10, Tarquini teaches the method according to claim 1, wherein said scanning and determining steps are implemented using a scan daemon (¶ 40-41).

12. In reference to claims 13,15,16,19-22, these claims are system claims that correspond to the method claims of claims 1,3,4,7,9,10. Therefore, claims 13,15,16,19-22 are rejected based upon the same rationale as given for claims 1,3,4,7,9,10 above.

13. In reference to claims 25,27,28,31,33, these claims are product claims that correspond to the method claims of claims 1,3,4,7,9,10. Therefore, claims 25,27,28,31,33 are rejected based upon the same rationale as given for claims 1,3,4,7,9,10 above.

14. **Claims 2,14,26 rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini et al (US Patent Publication No 2003/0101353) in view of Copeland (US Patent No 7,185,368)**.

In reference to claims 2,14,26, Tarquini teaches the corresponding method, system, and product according to claims 1,13,25 respectively, wherein said at least one action is selected from the group consisting of:

interrupting transmission of any data packets determined to be malicious to said application layer of said network protocol, wherein the interrupting is performed prior to the first application processing the malicious data packets; logging of errors related to any data packets determined to be malicious (¶ 41);

informing a network administrator any data packets are determined to be malicious; intimating said transport layer terminate an existing connection related to any data packets determined to be malicious (¶ 48);

blocking network access to a source of any data packets determined to be malicious; terminating an application of an application layer if any data packets are determined to be malicious; and notifying an application of an application layer if any data packets are determined to be malicious (¶s 40-41).

Tarquini fails to explicitly teach modifying firewall rules of a host computer if any data packets are determined to be malicious. However, Copeland discloses an intrusion detection system that modifies a firewalls behavior by configuring the firewall to drop packets it finds to be malicious for the purpose of protecting a network from the harmful effects of a network intrusion (column 19 lines 20-30 & column 22 lines 40-48).

It would have been obvious for one of ordinary skill in the art to modify Vaidya by modifying firewall rules of a host computer if any data packets are determined to be malicious as per the teachings of Copeland for the purpose of protecting a network from the harmful effects of a network intrusion.

15. **Claims 11,23,34 rejected under 35 U.S.C. 103(a) as being unpatentable over Tarquini et al (US Patent Publication No 2003/0101353) in view of Triulzi et al (US Patent Publication No 2004/0117478)**.

16. In reference to claims 11,23,34, Tarquini teaches the corresponding method, system, and product according to claims 1,13,25 respectively. Tarquini fails to explicitly teach, further

comprising the step of the target computer system generating fake network accessible services. However, Triulzi discloses that generation of fake network data and services for the purpose of detecting and analyzing network attacks (¶s 67 and 133). It would have been obvious for one of ordinary skill in that art to modify Tarquini to further comprise the step of the target computer system generating fake network accessible services as per the teachings of Triulzi for the purpose of detecting and analyzing network attacks.

Conclusion

17. The above rejections are based upon the broadest reasonable interpretation of the claims. Applicant is advised that the specified citations of the relied upon prior art, in the above rejections, are only representative of the teachings of the prior art, and that any other supportive sections within the entirety of the reference (including any figures, incorporation by references, claims and/or priority documents) is implied as being applied to teach the scope of the claims.

18. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See attached Form 892.

19. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to RAMY M. OSMAN whose telephone number is (571)272-4008. The examiner can normally be reached on M-F 9-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ario Etienne can be reached on (571) 272-4001. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

RMO
March 26, 2008

/Ario Etienne/

Supervisory Patent Examiner, Art Unit 2157